Security Management Server Virtual

Guia de instalação e início rápido v10.1

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam você a usar melhor o seu produto.

AVISO: Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.

ADVERTÊNCIA: Uma ADVERTÊNCIA indica possíveis danos à propriedade, risco de lesões corporais ou mesmo risco de vida.

2018 - 11

Rev. A01

Índice

1

Guia de Início Rápido

Este Guia de início rápido destina-se a usuários mais experientes com o objetivo de colocar o Dell Server em uso o mais rápido possível. Como regra geral, a Dell recomenda instalar o Dell Server primeiro, seguido pela instalação dos clientes.

Para obter instruções mais detalhadas, consulte o Guia de instalação do Security Management Server Virtual.

Para obter informações sobre pré-requisitos do Dell Server, consulte Dell Server, Pré-requisitos do Management Console e Pré-requisitos do Proxy Mode.

Para obter informações sobre como atualizar um Dell Server existente, consulte Update Security Management Server Virtual.

Installation

1 Navegue até o diretório no qual os arquivos do Dell Data Security estão armazenados e clique duas vezes para importar para o VMware o Servidor de gerenciamento de segurança virtual **v10.x.x Build x.ova**.

   NOTA: OVA agora está assinado por SHA256 e a importação falhará dentro do VMware thick client. Para formação consulte https://kb.vmware.com/s/article/2151537 .

2 Ligue o Security Management Server Virtual

3 Siga as instruções na tela.

Configuration

Antes de ativar os usuários, é recomendável concluir as seguintes tarefas de configuração no Terminal do Servidor de gerenciamento de segurança virtual:

- Definir as configurações do SMTP
- Importar um certificado existente ou inscrever um novo certificado de servidor
- Atualizar o Security Management Server Virtual
- Instale um cliente FTP que ofereça suporte para o protocolo SFTP na porta 22 e configure os usuários de FTP.

  Se sua organização tiver dispositivos voltados para a área externa, consulte Instalar e configurar o modo proxy.

Abrir o Management Console

Abra o Management Console neste endereço: https://server.domain.com:8443/webui/

As credenciais padrão são **superadmin/changeit**.

Para obter uma lista de navegadores da Web compatíveis, consulte Pré-requisitos do Management Console.

Tarefas administrativas

Se você não tiver iniciado o Management Console, faça-o agora. As credenciais padrão são **superadmin/changeit**.

A Dell recomenda que você atribua funções de administrador o quanto antes. Para concluir essa tarefa agora, consulte Atribuir Função de Dell Administrator.

Clique em "?" no canto superior do Management Console para iniciar a *AdminHelp*. A página *Introdução* é mostrada. Clique em **Adicionar domínio**.

As políticas de linha de base foram definidas para a sua organização, mas devem ser modificadas de acordo com as suas necessidades específicas, da seguinte maneira (o licenciamento e os direitos guiam todas as ativações):

- A criptografia com base na política será ativada com criptografia de chave comum
- Computadores com unidades de criptografia automática serão criptografados
- O BitLocker Management não é ativado
- O Advanced Threat Prevention não é ativado
- O Threat Protection é desativado
- A mídia externa não será criptografada
- As portas não serão gerenciadas pelo controle de porta
- Dispositivos com criptografia completa de disco instalada não serão criptografados
- O Data Guardian é desativado

Veja o tópico *Gerenciar políticas* da AdminHelp para navegar para os grupos de tecnologia e obter as descrições das políticas.

As tarefas de início rápido estão concluídas.

2

Guia de instalação detalhada

Este Guia de Instalação tem como objetivo ajudar usuários menos experientes com a instalação e configuração do Servidor de gerenciamento de segurança virtual. Como regra geral, a Dell recomenda instalar o Servidor de gerenciamento de segurança virtual primeiro, seguido pela instalação dos clientes.

Para obter informações sobre como atualizar um Servidor de gerenciamento de segurança virtual existente, consulte Update Security Management Server Virtual.

Sobre o Servidor de gerenciamento de segurança virtual

O Management Console permite monitorar o estado de pontos finais, a aplicação de políticas e a proteção em toda a empresa. O modo Proxy oferece uma opção de modo DMZ de front-end para uso com o Servidor de gerenciamento de segurança virtual.

O Servidor de gerenciamento de segurança virtual tem os seguintes recursos:

- Gerenciamento centralizado de até 3.500 dispositivos
- Criação e gerenciamento de política de segurança baseada em função
- Recuperação de dispositivo auxiliado pelo administrador
- Separação de deveres administrativos
- Distribuição automática de políticas de segurança
- Caminhos confiáveis para comunicação entre os componentes
- Geração de chave de criptografia exclusiva e depósito de chave de segurança
- Auditoria e relatórios de compatibilidade centralizados
- Autogeração de certificados autoassinados

Entre em contato com o Dell ProSupport

Ligue para 877-459-7304, extensão 4310039 para obter suporte por telefone, 24 horas por dia, 7 dias na semana, para o seu produto Dell.

Há também disponível o serviço de suporte on-line para os produtos Dell no site dell.com/support. O suporte on-line inclui drivers, manuais, orientações técnicas, perguntas frequentes e problemas emergentes.

Quando telefonar, tenha em mãos a Etiqueta de serviço ou Código de serviço expresso, para nos ajudar a garantir que possamos direcioná-lo rapidamente ao especialista técnico correto.

Para obter os números de telefone fora dos Estados Unidos, veja Números de telefone internacionais do Dell ProSupport.

Requisitos

Servidor de gerenciamento de segurança virtual

Hardware

O espaço em disco recomendado para o Servidor de gerenciamento de segurança virtual é de 80 GB.

Ambiente virtualizado

O Servidor de gerenciamento de segurança virtual v10.1 foi validado com os seguintes ambientes virtualizados.

Atualmente, a Dell oferece suporte à hospedagem do Dell Security Management Server ou Dell Security Management Server Virtual dentro de um ambiente de IaaS (Infrastructure as a Service, infraestrutura como serviço) hospedado na nuvem, tal como Amazon Web Services, Azure e vários outros provedores. O suporte a esses ambientes somente será limitado pela funcionalidade do servidor do aplicativo hospedado nessas máquinas virtuais; a administração e a segurança dessas máquinas virtuais ficarão a cargo do administrador da solução IaaS.

Os requisitos de infraestrutura adicionais (Active Directory, além de SQL Server para o Dell Security Management Server) ainda são necessários para permitir o funcionamento correto.

Ambientes virtualizados

- VMware Workstation 12.5
  - CPU de 64 bits necessária
  - 8 GB de RAM recomendado
  - 80 GB de espaço no disco rígido
  - Computador host com no mínimo dois núcleos
  - Consulte a página http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obter uma lista completa dos sistemas operacionais host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Consulte https://kb.vmware.com/s/article/1003746 para obter mais informações

- VMware Workstation 14.0
  - CPU de 64 bits necessária
  - 8 GB de RAM recomendado
  - 80 GB de espaço no disco rígido
  - Computador host com no mínimo dois núcleos
  - Consulte a página http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obter uma lista completa dos sistemas operacionais host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Consulte https://kb.vmware.com/s/article/1003746 para obter mais informações

- VMware Workstation 14.1
  - CPU de 64 bits necessária
  - 8 GB de RAM recomendado
  - 80 GB de espaço no disco rígido
  - Computador host com no mínimo dois núcleos
  - Consulte a página http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obter uma lista completa dos sistemas operacionais host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Consulte https://kb.vmware.com/s/article/1003746 para obter mais informações

- VMware ESXi 6.5
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - 80 GB de espaço no disco rígido
  - Não é necessário ter um sistema operacional específico
  - Consulte a página http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para ver uma lista completa de sistemas operacionais do host compatíveis

- O hardware precisa estar em conformidade com os requisitos mínimos do VMware
- Consulte https://kb.vmware.com/s/article/1003746 para obter mais informações

- VMware ESXi 6.0
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - 80 GB de espaço no disco rígido
  - Não é necessário ter um sistema operacional específico
  - Consulte a página http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para ver uma lista completa de sistemas operacionais do host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Consulte https://kb.vmware.com/s/article/1003746 para obter mais informações

- VMware ESXi 5.5
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - 80 GB de espaço no disco rígido
  - Não é necessário ter um sistema operacional específico
  - Consulte a página http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para ver uma lista completa de sistemas operacionais do host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Consulte https://kb.vmware.com/s/article/1003746 para obter mais informações

- Hyper-V Server (instalação completa ou básica)
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - 80 GB de espaço no disco rígido
  - Não é necessário ter um sistema operacional
  - O hardware precisa estar em conformidade com os requisitos mínimos do Hyper-V
  - Deve ser executado como uma máquina virtual da geração 1

NOTA: Parar obter informações sobre como configurar o Hyper-V, siga as instruções para sistemas operacionais de endpoint: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v ou para sistemas operacionais de servidor: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server.

Management Console

Navegadores de Internet

NOTA:
O navegador precisa aceitar cookies.

A tabela a seguir detalha os navegadores de Internet suportados.

Navegadores de Internet

- Internet Explorer 11.x ou posterior
- Mozilla Firefox 41.x ou posterior
- Google Chrome 46.x ou posterior

Modo Proxy

Hardware

A tabela a seguir detalha os requisitos *mínimos* de hardware.

Processador

CPU Dual-Core moderna (1,5 Ghz +)

RAM

No mínimo 2 GB dedicados de RAM/4 GB dedicados de RAM recomendados

Espaço livre em disco

1,5 GB de espaço livre em disco (além do espaço de paginação virtual)

Placa de rede

Placa de interface de rede 10/100/1000

Diversos

IPv4, IPv6 ou uma combinação de IPv4 e IPv6 são compatíveis

Software

A tabela a seguir detalha o software que já precisará estar instalado antes da instalação do modo Proxy.

Pré-requisitos

- **Windows Installer 4.0 ou posterior**

  O Windows Installer 4.0 ou posterior deve ser instalado no servidor no qual a instalação está sendo feita.

- **Pacote Redistribuível do Microsoft Visual C++ 2010**

  Se não estiver instalado, o instalador realizará o processo para você.

- **Microsoft .NET Framework versão 4.5.2**

  A Microsoft publicou as atualizações de segurança para o .NET Framework versão 4.5.2

NOTA:

O UAC (Universal Account Control, controle de conta universal) deve ser desativado quando a instalação ocorrer em um diretório protegido. Após desativar o UAC, o servidor precisa ser reiniciado para que essa alteração tenha efeito.

Local de registro para Windows Servers: HKLM\SOFTWARE\Dell.

A tabela a seguir detalha os requisitos de software para o servidor no modo Proxy.

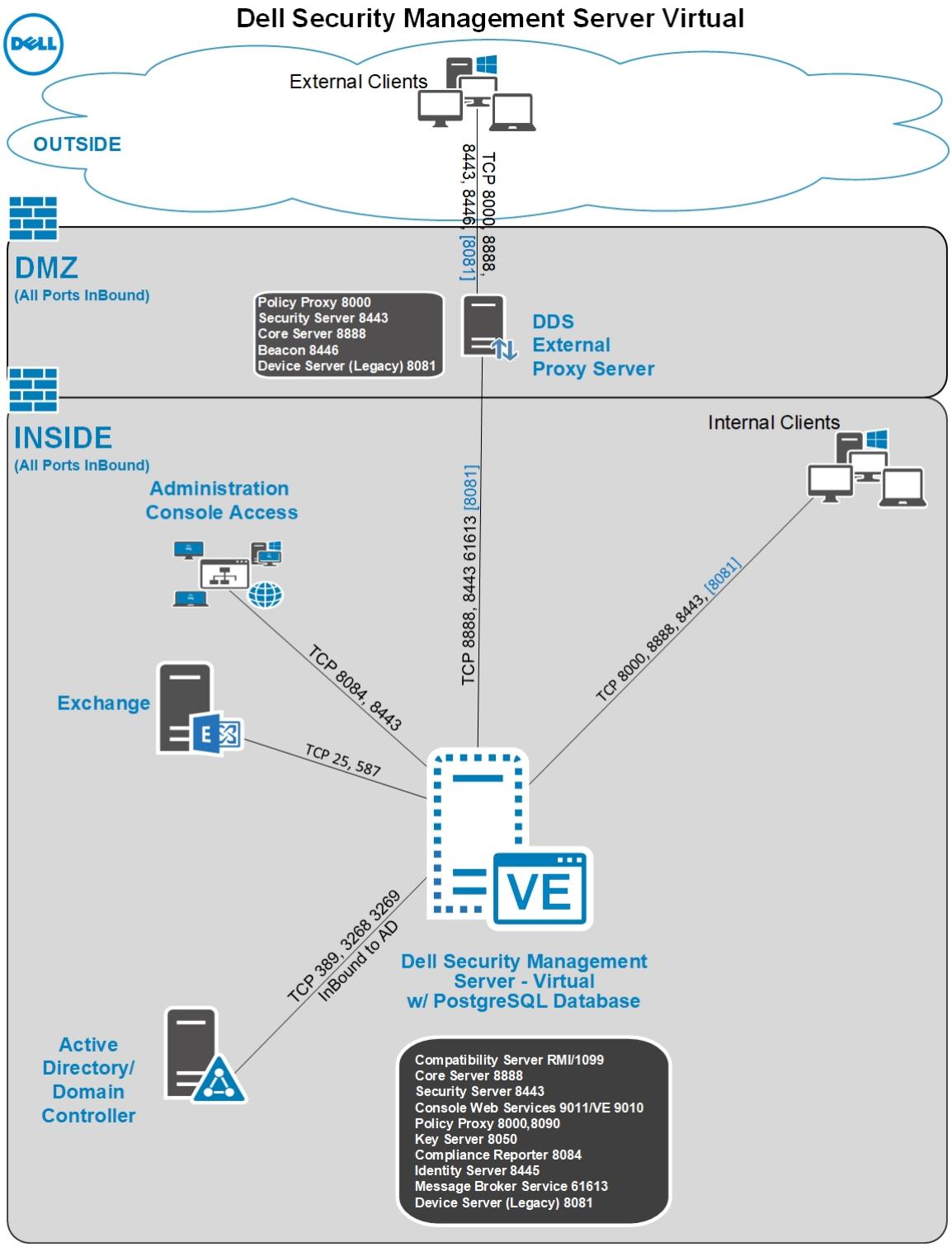
Sistema operacional
• **Windows Server 2016** - Standard Edition - Datacenter Edition • **Windows Server 2012 R2** - Standard Edition - Datacenter Edition • **Windows Server 2008 R2 SP0-SP1 64 bits** - Standard Edition - Enterprise Edition

Design da arquitetura do Security Management Server Virtual

As soluções do Dell Encryption, Endpoint Security Suite Enterprise e Data Guardian, são produtos altamente dimensionáveis, de acordo com a quantidade de endpoints que se deseja criptografar na sua organização.

Componentes da arquitetura

Abaixo encontra-se uma implementação básica para o Dell Security Management Server Virtual.



Fazer download e instalar o arquivo OVA

Na instalação inicial, o Servidor de gerenciamento de segurança virtual é fornecido como um arquivo OVA (Open Virtual Application), um aplicativo virtual aberto usado para oferecer softwares que são executados em uma máquina virtual. O arquivo OVA está disponível em www.dell.com/support, nas páginas de suporte dos seguintes produtos do Dell Data Security:

- Criptografia

- Endpoint Security Suite Enterprise
- Data Guardian

Para fazer download do arquivo OVA:

1 Navegue até a página *Drivers e downloads* do produto apropriado listado acima.
2 Clique em **Drivers e downloads**.
3 Selecione a versão apropriada do VMware ESXi.
4 Faça download do pacote adequado.

Para instalar o arquivo OVA:

Antes de começar, verifique se todos os requisitos de ambiente virtual e do sistema são atendidos.

1 Na mídia de instalação da Dell, localize o *Security Management Server Virtual v9.x.x versão x.ova* e clique duas vezes para importar para o VMware.

NOTA: Se você estiver usando o Hyper-V em vez do VMware, siga as instruções para Windows 10 https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/. Para os sistemas operacionais baseados em servidor, siga as instruções: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server. Se estiver usando o ESXi em vez do VMware, siga as instruções:https://kb.vmware.com/s/article/2109708 .

2 Siga as instruções na tela.

NOTA: Se a importação falhar ao usar o VMware, então o cliente da Web é o caminho sugerido para a importação do arquivo OVA. Para obter mais informações, consulte https://kb.vmware.com/s/article/2151537.

3 Ligue o Servidor de gerenciamento de segurança virtual.
4 Selecione o idioma para o contrato de licença e selecione **Mostrar EULA**.
5 Leia o contrato e selecione **Aceitar EULA**.
6 Se houver uma atualização disponível, selecione **Aceitar**.
7 Selecione **Modo Conectado** ou **Modo Desconectado**.

NOTA:
Se você selecionar **Modo desconectado**, ele nunca poderá ser alterado para Modo conectado.

O Modo Desconectado isola o Dell Server da Internet e de uma LAN não protegida ou outra rede. Todas as atualizações devem ser realizadas manualmente. Para obter mais informações sobre as políticas e o Modo desconectado, consulte o tópico *AdminHelp*.

8 Em *Definir senha do ddguser*, digite a senha (padrão) atual, **ddguser** e, em seguida, insira uma senha única, digite-a novamente e selecione **Aplicar**.

As senhas precisam conter o seguinte:

- Pelo menos 8 caracteres
- Pelo menos 1 letra maiúscula
- Pelo menos 1 número
- Pelo menos 1 caractere especial

NOTA: É possível manter a senha padrão, selecionando Cancelar ou pressionando Esc no teclado.

9 Selecione **Fechar** para entrar na tela para configurar a janela do nome de host.
10 Em *Configurar nome de host*, use a tecla de espaço para remover o nome de host padrão. Digite um nome de host único e selecione **OK**.
11 Em *Definir configurações da rede*, selecione qualquer uma das opções abaixo e selecione **OK**.

- (Padrão) Usar o DHCP (IPv4)

- (Recomendado) No campo *Usar DHCP*, pressione a barra de espaço para remover o X e digite esses endereços manualmente, conforme necessário:

  IP estático

  Máscara de rede

  Gateway padrão

  Servidor DNS 1

  Servidor DNS 2

  Servidor DNS 3

  IPv6 ou IPv4 podem ser selecionados para uma configuração estática.

- **NOTA: Quando um IP estático é usado, é necessário também criar uma entrada de host no servidor DNS.**

12 No prompt de confirmação do fuso horário, selecione **OK**.

13 Quando a mensagem exibida indicar que a configuração inicial foi concluída, selecione **OK**.

14 Definir as configurações do SMTP.

15 Importar um certificado existente ou inscrever um novo certificado de servidor.

16 Atualizar o Security Management Server Virtual.

17 Instale um cliente FTP que ofereça suporte para o protocolo SFTP na porta 22 e configure os usuários de FTP.

As tarefas de instalação do Servidor de gerenciamento de segurança virtual estão completas.

Abrir o Management Console

Abra o Management Console neste endereço: https://server.domain.com:8443/webui/

As credenciais padrão são **superadmin/changeit**.

Para obter uma lista de navegadores da Web compatíveis, consulte Pré-requisitos do Management Console.

Instalar e configurar o modo Proxy

Modo Proxy fornece uma opção de front-end (Modo DMZ) para uso com o Dell Server. Se você pretende implementar componentes da Dell no DMZ, verifique se eles estão devidamente protegidos contra ataques.

NOTA: O serviço de beacon é instalado como parte desta instalação para oferecer suporte ao beacon de retorno de chamada do Data Guardian, que insere um beacon de retorno de chamada em cada arquivo protegido pelo Data Guardian ao permitir ou impor Documentos protegidos do Office no ambiente. Isso permite a comunicação entre qualquer dispositivo em qualquer local e o servidor front-end. Verifique se a segurança da rede necessária está configurada antes de usar o sinalizador de retorno de chamada.

Para executar a instalação, é necessário ter o nome de host totalmente qualificado do servidor DMZ.

1 Na mídia de instalação Dell, navegue até o diretório do Servidor de gerenciamento de segurança. **Descompacte** (NÃO copie/cole nem arraste/solte) o Servidor de gerenciamento de segurança-x64 no diretório raiz do servidor onde você está instalando o Servidor de gerenciamento de segurança virtual. ***Copiar/colar ou arrastar/soltar produz erros e causa uma instalação malsucedida.***

2 Clique duas vezes em **setup.exe**.

3 Selecione o idioma para a instalação e clique em **OK**.

4 Se os pré-requisitos ainda não estiverem instalados, será mostrada uma mensagem informando quais pré-requisitos serão instalados. Clique em **Instalar**.

5 Clique em **Avançar** na caixa de diálogo de Boas-vindas.

6 Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.

7 Digite a Chave do Produto de 32 caracteres e, em seguida, clique em **Avançar**. A Chave do Produto está localizada no arquivo EnterpriseServerInstallKey.ini.

8 Selecione **Instalação do front-end** e clique em **Avançar**.

9 Para instalar o servidor de front-end no local padrão C:\Program Files\Dell, clique em **Avançar**. Caso contrário, clique em **Alterar** para selecionar outro local e clique em **Avançar**.

10 Você pode escolher entre alguns tipos de certificados digitais para usar.

NOTA: É extremamente recomendado o uso de um certificado digital de uma autoridade de certificação confiável.

Selecione a opção “a” ou “b” abaixo:

a Para usar um certificado existente que foi comprado de uma autoridade de certificação, selecione **Importar um certificado existente** e clique em **Avançar**.

b Para criar um certificado autoassinado, selecione **Criar um certificado autoassinado e importá-lo para o armazenamento de chaves e clique em Avançar.**

Na caixa de diálogo *Criar certificado autoassinado*, digite as informações a seguir:

Nome do computador totalmente qualificado (exemplo: nomedocomputador.domínio.com)

Organização

Unidade organizacional (exemplo: Segurança)

Cidade

Estado (nome completo)

País: abreviação com duas letras

Clique em **Avançar**.

NOTA: Por padrão, o certificado expira em um 10 anos.

11 Na caixa de diálogo *Configuração do servidor de front-end*, digite o nome de host ou o alias do DNS do servidor de back-end, selecione **Dell Security Management Server** e clique em **Avançar**.

12 Na caixa de diálogo *Configuração de instalação do servidor de front-end*, você pode ver ou editar os nomes de host e as portas.

- Para aceitar os nomes de host e as portas padrão, na caixa de diálogo *Configuração de instalação do servidor de front-end*, clique em **Avançar**.
- Para ver ou editar os nomes de host, na caixa de diálogo *Configuração do servidor de front-end*, clique em **Editar nomes de host**. Edite os nomes de host apenas se necessário. A Dell recomenda usar as configurações padrão.

NOTA:
Um nome de host não pode conter um caractere sublinhado ("_").

Desmarque um proxy apenas se tiver certeza de que não quer configurá-lo para instalação. Se você desmarcar um proxy nessa caixa de diálogo, ele não é instalado.

Quando concluído, clique em **OK**.

- Para ver ou editar as portas, na caixa de diálogo *Configuração do servidor de front-end* clique em **Editar portas externas** ou **Editar portas de conexão internas**. Edite as portas apenas se necessário. A Dell recomenda usar as configurações padrão.

Se você desmarcar um proxy na caixa de diálogo *Editar nomes de host do front-end*, sua porta não será mostrada nas caixas de diálogo Portas externas ou Portas internas.

Quando concluído, clique em **OK**.

13 Na caixa de diálogo *Pronto para instalar o programa*, clique em **Instalar**.

14 Ao terminar a instalação, clique em **Concluir**.

Tarefas básicas de configuração do terminal do

As tarefas de configuração básica são acessadas pelo menu principal.

Verifcar Painel de sistema

Para verificar o status dos serviços do Dell Server, no menu principal, selecione **Painel de sistema**.

O widget *Informações do sistema* exibe versão atual, nome de host, endereço ip, assim como uso de cpu, memória e disco.

O widget *Histórico da versão* exibe alterações ao esquema do banco de dados, por versão. Os dados são fornecidos pela tabela "informações" e são classificados por hora, com a versão mais recente na parte superior.

A tabela a seguir descreve cada serviço e sua função no widget *Integridade do serviço*.

Nome	Descrição
Message Broker	Enterprise Server Bus
Identity Server	Processa as solicitações de autenticação de domínio.
Compatibility Server	Um serviço para gerenciar a arquitetura corporativa.
Security Server	Fornece o mecanismo para controlar comandos e a comunicação com o Active Directory.
Compliance Reporter	Fornece uma visão completa do ambiente para auditoria e geração de relatórios de conformidade.
Core Server	Um serviço para gerenciar a arquitetura corporativa. Esse serviço também lida com todas as ativações, política e coleta de inventário de dispositivos com base em "Agent".
Core Server HA (Alta disponibilidade)	Um serviço de alta disponibilidade que permite uma maior segurança e desempenho das conexões de HTTPS ao se gerenciar a arquitetura corporativa.
Inventory Server	Processa a fila de inventário.
Forensic Server	Oferece serviços da Web para a API forense.
Policy Proxy	Fornece um caminho de comunicação baseado na rede para fornecer atualizações da política de segurança e atualizações de inventário.

Os serviços são monitorados e reiniciados automaticamente, caso necessário.

NOTA: Se o processo do personalizador de banco de dados falhar, os servidores passarão para o estado Falha na execução. Para verificar o log do personalizador de banco de dados, no menu principal, selecione Ver logs.

Alterar Nome de host

Essa tarefa pode ser executada a qualquer momento. Não é necessário começar a usar o Servidor de gerenciamento de segurança virtual.

1 No menu *Configuração básica*, selecione **Nome do host**.
2 Use a tecla de espaço para remover o nome do host existente, substitua-o por um novo nome de host e selecione **OK**.

Alterar configurações de rede

Essa tarefa pode ser executada a qualquer momento. Não é necessário começar a usar o Servidor de gerenciamento de segurança virtual.

1 No menu *Configuração básica*, selecione **Rede**.
2 Na tela *Definir configurações da rede*, selecione qualquer uma das opções abaixo e selecione **OK**.
   - (Padrão) Usar o DHCP (IPv4).
   - (Recomendado) No campo *Usar DHCP*, pressione a barra de espaço para remover o X e digite esses endereços manualmente, conforme necessário:

     IP estático

     Máscara de rede

     Gateway padrão

     Servidor DNS 1

     Servidor DNS 2

     Servidor DNS 3

     IPv6 ou IPv4 podem ser selecionados para uma configuração estática.

   NOTA:
   Ao usar um IP estático, você precisa criar uma entrada de host no servidor DNS.

Definir suporte ao servidor DMZ

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o Servidor de gerenciamento de segurança virtual.

1 No menu *Configuração básica*, selecione **Suporte do servidor DMZ**.
2 Use a barra de espaço para inserir um **X** no campo Habilitar suporte do servidor DMZ
3 Informe o nome de domínio totalmente qualificado do servidor DMZ e selecione **OK**.

NOTA: Para utilizar um servidor DMZ, consulte as instruções de instalação para um servidor proxy acima Instalar e configurar o modo Proxy.

Alterar o fuso horário

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o Servidor de gerenciamento de segurança virtual.

1 No menu *Configuração básica*, selecione **Fuso horário**.
2 Na tela *Fuso horário*, use as teclas de seta para selecionar o fuso horário e, em seguida, selecione **Entrar**.

Atualizar o Servidor de gerenciamento de segurança virtual

Para obter mais informações sobre uma atualização específica, consulte os avisos técnicos do *Servidor de gerenciamento de segurança virtual*, localizados em dell.com/support. Para ver a versão e a data de instalação de uma atualização que já é aplicada, verifique o *Painel de sistema*.

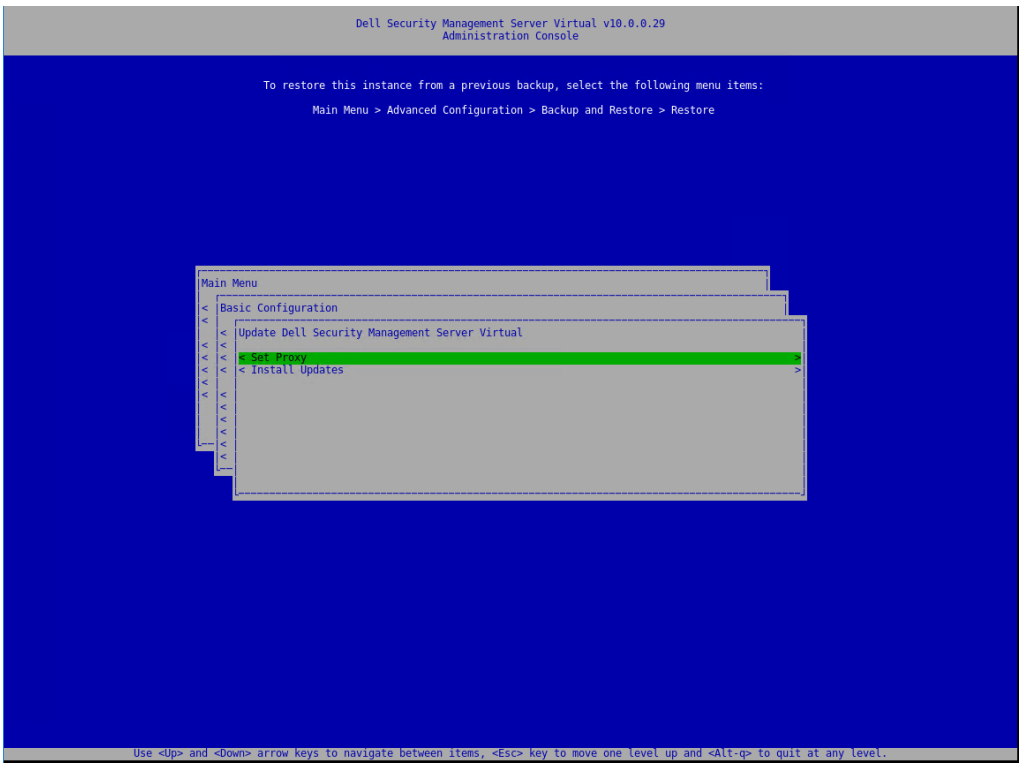
Para receber notificações por e-mail quando atualizações do Dell Server forem disponibilizadas, consulte Definir as configurações de SMTP.

Se forem realizadas alterações na política, mas não confirmadas no Management Console, aplique as alterações de política antes de atualizar o Dell Server:

1 Como um administrador Dell, faça login no Management Console.
2 No menu à esquerda, clique em **Gerenciamento** > **Confirmar**.
3 Digite uma descrição da alteração no campo Comentário.
4 Clique em **Confirmar políticas**.
5 Quando a confirmação for concluída, faça logoff do Management Console.

Atualizar o Servidor de gerenciamento de segurança virtual (modo Conectado)

1 A Dell recomenda a execução de um backup regular. Antes de atualizar, certifique-se de que o processo de backup esteve funcionando corretamente. Consulte Backup e restauração.
2 No menu **Configuração básica**, selecione **Atualizar o Dell Security Management Server Virtual**.



NOTA: O número da versão pode ser diferente da captura de tela anexa.

3 Selecione a ação desejada:

- Definir as configurações de proxy – Selecione esta opção para definir as configurações de proxy para as atualizações sendo baixadas.

  Na tela *Definir as configurações de proxy*, pressione a barra de espaço para inserir um **X** no campo *Usar proxy*. Digite os dados HTTPS e HTTP. Se for necessária a autenticação do firewall, pressione a barra de espaço para inserir um **X** no campo Autenticação necessária. Digite seu nome de usuário e sua senha e clique em **OK**.

  NOTA: Essa opção Definir proxy agora também atualiza as configurações de proxy para os vários aplicativos baseados em Java, para obtenção de licenças "on-the-box", bem como comunicação com o Endpoint Security Suite Enterprise SaaS e a infraestrutura de back-end Dell/Credant.

- Instalar atualizações - Na versão 9.11 e posterior, ao selecionar **Instalar atualizações**, vários repositórios Ubuntu genéricos são consultados, juntamente com dist.ddspproduction.com. O dist.ddspproduction.com é um repositório personalizado da Dell que contém as atualizações de aplicativos do Dell Security Management Server. Estes repositórios são consultados por meio de DNS com a porta 53 para os servidores DNS definidos na *Configuração de rede* ou são obtidos por meio de DHCP. Assim que o servidor resolve essas conexões, a Dell conecta pela porta 443 para o dist.ddspproduction.com e pela porta 80 para todas as atualizações do Ubuntu. A Dell baixa todas as atualizações que estão disponíveis. As configurações de proxy definidas em *Definir proxy* são usadas para conexões para download nas portas 443 e 80.

Atualizar o Servidor de gerenciamento de segurança virtual (modo Desconectado)

1 A Dell recomenda a execução de um backup regular. Antes de atualizar, certifique-se de que o processo de backup esteve funcionando corretamente. Consulte Backup e restauração.

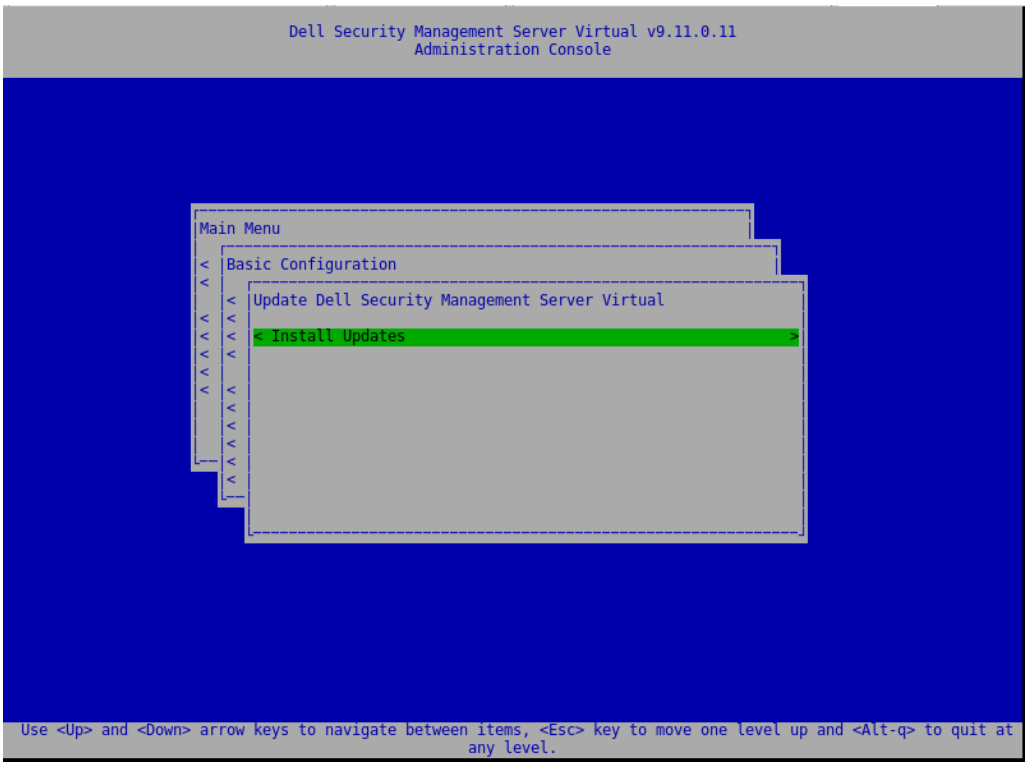
2 No Dell ProSupport, obtenha o arquivo .deb que contém a atualização mais recente do Dell Server.

3 Armazene o arquivo .deb na pasta /updates no servidor FTP seguro do Dell Server.

Certifique-se de que o cliente FTP ofereça suporte para o SFTP na porta 22 e que um usuário FTP esteja configurado. Consulte Configurar usuários de FTP.

4 No menu **Configuração básica**, selecione **Atualizar o Security Management Server Virtual**.

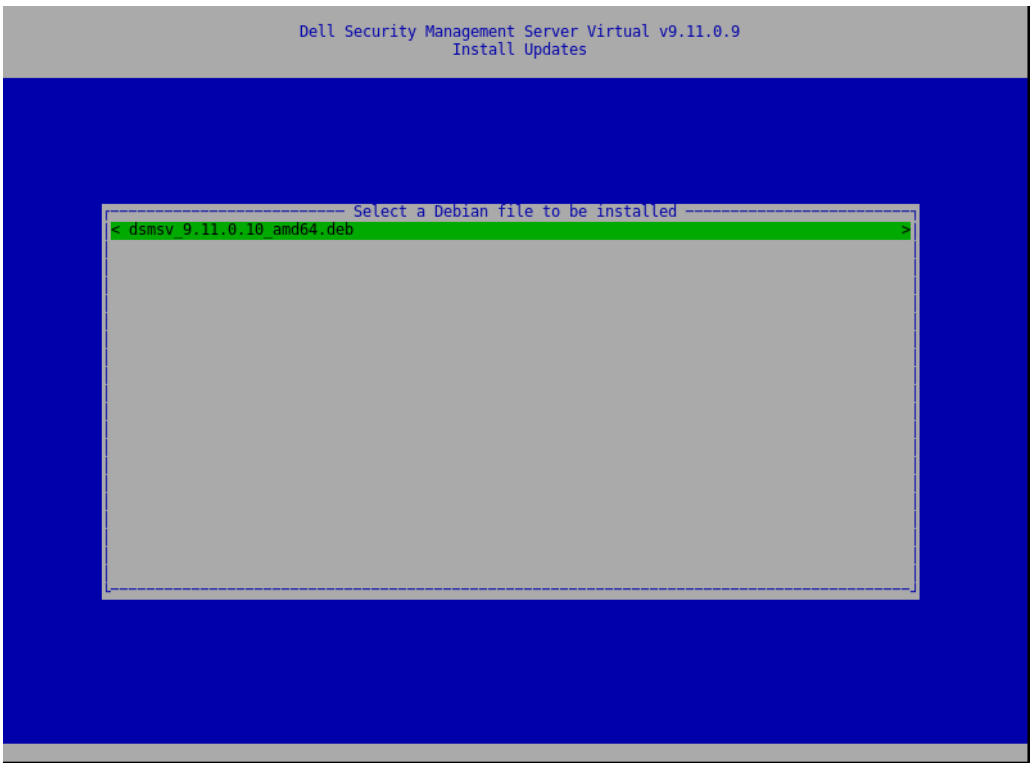
5 Selecione **Instalar atualização** e pressione a tecla **Enter**.



NOTA: O número da versão pode ser diferente da captura de tela anexa.

Se o arquivo .deb não for exibido, verifique se esse arquivo está armazenado no local correto.

6 Selecione o arquivo de atualização .deb que você deseja instalar e pressione a tecla **Enter**.



NOTA: O número da versão pode ser diferente da captura de tela anexa.

Alterar senhas de usuário

Essa tarefa pode ser executada a qualquer momento. Não é necessário começar a usar o Servidor de gerenciamento de segurança virtual.

Você pode alterar senhas para esses usuários:

- delluser (Administrador do terminal) - Este usuário tem acesso ao terminal e aos menus do Dell Server.
- dellconsole (acesso shell) - Este usuário tem acesso shell ao Dell Server. O acesso ao shell está disponível para um administrador de rede a fim de verificar e solucionar problemas de conectividade de rede.
- dellsupport (Administrador do Dell ProSupport) – Este usuário tem direitos de "sudo" e deve ser usado com moderação. Para fins de segurança, você controla a senha para esta conta.

1 No menu *Configuração básica*, selecione **Alterar senhas de usuário**.
2 Na tela *Alterar senhas de usuário*, selecione a senha de usuário que será alterada e selecione **Entrar**.
3 Na tela *Definir senha*, insira a senha atual, insira a nova senha, insira a nova senha de novo e selecione **OK**.
As senhas precisam conter o seguinte:

- Pelo menos 8 caracteres
- Pelo menos 1 letra maiúscula
- Pelo menos 1 número
- Pelo menos 1 caractere especial

NOTA:
Para escolher diferentes contas de usuário, use a "barra de espaço" no teclado para mostrar a lista de seleção.

Configurar usuários de Secure File Transfer (SFTP)

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o Servidor de gerenciamento de segurança virtual.

1 No menu *Configuração básica*, selecione **SFTP**.
2 Na tela *SFTP*, para adicionar um usuário SFTP e definir uma senha, pressione **Enter** ou a tecla de seta para abaixo no campo *Status* para o usuário. Ao pressionar a barra de espaços, você tem a opção de atualizar ou excluir um usuário existente. Para desativar um usuário SFTP, selecione **Apagar** depois de escolher o usuário e, em seguida, selecione **Sim** na tela de confirmação SFTP.
3 Informe um nome de usuário e uma senha para o usuário SFTP.
As senhas precisam conter o seguinte:

- Pelo menos 8 caracteres
- Pelo menos 1 letra maiúscula
- Pelo menos 1 número
- Pelo menos 1 caractere especial

4 Quando terminar de inserir os usuários SFTP, selecione **Aplicar**.

Habilitar o SSH

Essa tarefa pode ser executada a qualquer momento. Não é necessário começar a usar o Servidor de gerenciamento de segurança virtual.

Você pode ativar o SSH para o login do administrador de suporte, acesso ao shell e a interface de linha de comando do terminal.

1 No menu *Configuração básica*, selecione **SSH**.
2 Selecione o usuário para o qual deseja habilitar o SSH, pressione a barra de espaço para inserir um **X** e selecione **OK**.

Iniciar ou parar serviços

Execute esta tarefa somente se for necessário.

1 Para iniciar ou parar simultaneamente todos os serviços, no menu *Configuração básica*, selecione **Iniciar aplicativo** ou **Parar aplicativo**.
2 Na janela de confirmação, selecione Sim.

NOTA:
As alterações no estado do servidor poderão levar até dois minutos para serem concluídas.

Reinicializar o dispositivo

Execute esta tarefa somente se for necessário.

1 No menu *Configuração básica*, selecione **Reinicializar o dispositivo**.
2 Na janela de confirmação, selecione Sim.
3 Depois de reiniciar, faça login no Servidor de gerenciamento de segurança virtual.

Desligar o dispositivo

Execute esta tarefa somente se for necessário.

1 No menu *Configuração básica*, desça e selecione **Encerrar dispositivo**.
2 Na janela de confirmação, selecione Sim.
3 Depois de reiniciar, faça login no Servidor de gerenciamento de segurança virtual.

Tarefas de configuração avançadas do terminal

As tarefas de configuração avançadas são acessadas no menu principal.

Configurar a rotação de log

NOTA: As instruções abaixo definem os arquivos de log que serão rodados para os aplicativos no Dell Security Management Server Virtual que suportam a rotação de log.

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o Servidor de gerenciamento de segurança virtual.

A rotação de log diária é ativada por padrão. Para alterar a rotação de log padrão, no menu *Configuração avançada*, selecione **Configuração de rotação de log**.

Para desativar a rotação de log, use a barra de espaço para inserir um **X** no campo *Sem rotação* e selecione **OK**.

Para ativar a rotação de log, siga essas etapas:

1 Para ativar a rotação diária, semanal ou mensal, use a barra de espaço para inserir um **X** no campo adequado. Para rotação semanal, use o menu suspenso para selecionar o dia apropriado da semana. Para rotação mensal, insira o dia apropriado do mês.
2 Informe um horário para a rotação no campo *Horário da rotação de log*.
3 Selecione **OK**.

Backup e restauração

Os backups podem ser configurados ou executados a qualquer momento e não são necessários para começar a usar o Servidor de gerenciamento de segurança virtual. A Dell recomenda que você configure um processo de backup regular. Para obter mais informações, consulte http://www.dell.com/support/article/us/en/19/sln304943/how-to-back-up-and-restore-dell-security-management-server-virtual-dell-data-protection-virtual-edition?lang=en

Quando armazenados no Dell Server e o disco atingir 90% da capacidade, nenhum backup novo será armazenado. Se as notificações por e-mail foram configuradas, você receberá uma notificação por e-mail informando que há pouco espaço de alocação em disco.

NOTA:
Para preservar o espaço em partição no disco e evitar o apagamento automático dos backups, remova os backups desnecessários do armazenamento.

Por padrão, os backups são executados diariamente. A Dell recomenda armazenar backups em um servidor FTP seguro externo em uma frequência que atenda às exigências da organização quanto aos backups e ao uso apropriado do espaço de armazenamento.

Para configurar uma programação de backup, no menu *Configuração avançada*, selecione **Backup e restauração > Configuração** e siga essas etapas:

1 Para ativar backups diários, semanais ou mensais, use a barra de espaço para inserir um **X** no campo adequado. Para ativar os backups semanalmente ou mensalmente, informe o dia adequado da semana ou o mês em formato de numeral, onde segunda=1. Para desativar os backups, use a barra de espaço para inserir um **X** no campo *Sem backups* e selecione **OK**.

2 Informe um horário para o backup no campo *Horário do backup*.

3 Selecione **OK**.

Para executar um backup imediato, no menu *Configuração avançada*, selecione **Backup e restauração > Fazer backup agora**. Quando a confirmação de backup for mostrada, selecione **OK**.

NOTA:
Antes de iniciar uma operação de restauração, todos os serviços dos servidores do Dell Server precisam estar em execução. Verificar o status do servidor. Se nem todos os serviços estiverem em execução, reinicie os serviços. Para obter mais informações, consulte Iniciar ou parar os serviços. Comece a restaurar ***apenas*** quando ***todos*** os serviços estiverem em execução.

Para fazer a restauração a partir de um backup, no menu *Configuração avançada*, selecione **Backup e restauração > Restaurar** e selecione o arquivo de backup a ser restaurado. Na tela de confirmação, selecione **Sim**.

O backup é restaurado após a reinicialização.

Armazenar os backups em um servidor FTP seguro

Para armazenar os backups em um servidor FTP, o cliente FTP precisa suportar o SFTP na porta 22.

De acordo com os requisitos de backup da organização, os backups podem ser baixados das seguintes maneiras:

- Manualmente
- Através de script automatizado
- Através da solução de backup aprovada da organização

Para fazer download de backups usando a solução de backup da organização, obtenha instruções detalhadas por parte do seu fornecedor de soluções de backup.

NOTA:
O Dell Server é baseado no Linux Debian Ubuntu x64.

Faça login no Dell Server como ddpsupport e use o comando `sudo` para configurar a solução de backup:

`sudo` <instruções do fornecedor de soluções de backup>

Faça backup dos conteúdos das seguintes pastas:

/backup (obrigatório)

/certificados (altamente recomendado)

/suporte (opcional)

Quando o processo sudo for concluído, digite **exit** e pressione **Enter** até o prompt de login ser exibido.

Definir as configurações do SMTP

Para receber as notificações de e-mail **ou** usar o usar o Data Guardian, siga as etapas nesta seção para definir as configuração de SMTP. As notificações por e-mail do Dell Server informam os destinatário do Servidor da Dell os estados de erro de status, atualizações de senha, disponibilidade de atualizações do Dell Server e problemas de licença do cliente.

É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

Para definir as configurações de SMTP, siga as seguintes etapas:

1 No menu *Configuração avançada*, selecione **Notificações por e-mail**.
2 Na tela Notificações por e-mail, para habilitar os alertas por e-mail, pressione a barra de espaço para inserir um **X** no campo *Habilitar alertas por e-mail*.
3 Insira o nome do domínio totalmente qualificado do SMTP Server.
4 Informe a porta SMTP.
5 Informe o usuário SMTP
6 Informe a senha SMTP
7 No campo *Origem da notificação*, informe o ID da conta de e-mail que enviará as notificações por e-mail.
8 No campo *Enviar status do servidor para*, informe o ID da conta de e-mail envia as notificações de status. Os destinatários são separados por vírgula ou ponto-e-vírgula.
9 No campo *Enviar alterações de senha para*, informe o ID da conta de e-mail que envia as notificações de alteração de senha.
10 No campo *Enviar atualizações do software para*, informe o ID da conta de e-mail que envia as notificações de atualização do software.
11 No campo de *lembrete de Alerta de serviço*, para ativar os lembretes, pressione a barra de espaço para inserir um **X** e defina o intervalo do lembrete, em minutos. Um lembrete de Alerta de serviço será acionado quando o intervalo do lembrete passar após uma notificação ser enviada sobre um problema de saúde do sistema e o host ou o serviço permanecer no mesmo estado.
12 No campo Relatório de resumo, para ativar os relatórios de notificações, selecione o intervalo desejado (diário, semanal ou mensal) e pressione a barra de espaço para inserir um **X**.
13 Selecione **OK**.

Importar um certificado existente ou inscrever um novo certificado de servidor

Você pode importar um certificado existente ou criar uma solicitação de certificado por meio do do Servidor de gerenciamento de segurança virtual.

É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

Importar um certificado de servidor existente

1 Exporte o certificado existente e sua cadeia completa de confiança do armazenamento de chaves.

> **NOTA: Mantenha a senha de exportação, pois você irá usá-la ao importar o certificado para o do Servidor de gerenciamento de segurança virtual.**

2 No servidor FTP do Dell Server, armazene o certificado em **/certificados**.

3 No menu *Configuração avançada*, selecione **Certificados do servidor**.

4 Selecione **Importar certificado existente**.

5 Selecione um arquivo de certificado para ser instalado no do Dell Server.

6 Quando solicitado, informe a senha de exportação do certificado e selecione **OK**.

7 Quando a importação estiver concluída, selecione **OK**.

> **NOTA: Para obter mais informações, consulte http://www.dell.com/support/article/us/en/19/sln302996/dell-data-protection-virtual-edition-dell-security-management-server-virtual-manual-csr-creation-and-certificate-import?lang=en**

Inscrever um novo certificado de servidor

1 No menu *Configuração avançada*, selecione **Certificados do servidor**.

2 Selecione **Novo certificado de servidor**.

3 Selecione **Criar solicitação de certificado**.

4 Preencha os campos na tela *Gerar solicitação de certificado*:

- Nome do país: código de duas letras de país.
- *Estado/província*: digite o nome do estado ou da província sem abreviação (por exemplo, Texas).
- *Nome do local/cidade.* Digite o valor adequado (por exemplo, Dallas).
- *Organização*: digite o valor apropriado (por exemplo, Dell).
- *Unidade organizacional*: digite o valor apropriado (por exemplo, Segurança).
- *Nome comum:* especifique o nome de domínio totalmente qualificado do servidor no qual o do Dell Server está instalado. Este nome totalmente qualificado inclui o nome do host e o nome do domínio (por exemplo: domínio.com).
- *ID de e-mail*: informe o endereço de e-mail para o qual a sua CSR será enviada.

5 Siga o processo da sua organização para adquirir um certificado de servidor SSL de uma Autoridade de Certificado. Envie o conteúdo do arquivo da CSR para assinatura.

6 Ao receber o certificado assinado, exporte-o como um arquivo .p7b e baixe a cadeia completa de confiança no formato .der.

7 Faça cópias de backup do certificado e da cadeia de confiança.

8 Carregue o arquivo do certificado e sua cadeia completa de confiança no servidor FTP seguro do do Dell Server.

9 No menu *Configuração avançada*, selecione **Certificados do servidor**.

10 Selecione **Novo certificado de servidor**.

11 Selecione `Concluir inscrição de certificado`.

12 Selecione o arquivo de certificado para ser instalado no do Dell Server.

13 Se solicitado, digite a senha do certificado: **changeit**.

Para ativar a validação de confiança nos clientes do Encryption baseado no Windows, consulte Ativar a verificação de cadeia de confiança do gerenciador.

Criar e instalar um certificado autoassinado

NOTA: Os certificados autoassinados gerados por padrão são emitidos por 10 anos.

1 No menu *Configuração avançada* do Dell Server, selecione **Certificados do servidor**.
2 Selecione **Criar e instalar um certificado autoassinado.**
3 Para confirmar que você quer substituir o certificado pré-instalado por um novo certificado, clique em **Sim**.
4 Digite a senha do certificado: **changeit**.
5 Após o novo certificado ser instalado, selecione **OK** e espere que os serviços sejam reiniciados.

Os serviços são reiniciados automaticamente.

Habilitar acesso ao banco de dados

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o Servidor de gerenciamento de segurança virtual.

NOTA: A Dell recomenda que você ative o acesso ao banco de dados somente se necessário, e desative-o assim que for concluído.

1 No menu *Configuração avançada*, selecione **Acesso ao banco de dados**.
2 Use a barra de espaço para inserir um **X** no campo *Ativar acesso ao banco de dados* e selecione **OK**. Se a senha do banco de dados ainda não tiver sido configurada, um prompt para essa senha será exibido.
3 Digite a senha de banco de dados.
4 Redigite a senha de banco de dados.
Os componentes do aplicativo Dell Data Security param automaticamente.

Definir ou alterar o idioma do terminal

É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

1 No menu principal, selecione **Definir idioma**.
2 Use as teclas de seta para selecionar o idioma preferencial.

Ver logs

Para verificar os seguintes logs, no menu principal, selecione **Ver logs**.

- Logs do sistema
  - Log do Syslog
  - Log de e-mail
  - Log de autenticação do (SSH)
  - Log do Postgres
  - Log de monitoramento
- Logs de servidor
  - Message Broker

  - Identity Server
  - Compatibility Server
  - Security Server
  - Compliance Reporter
  - Core Server
  - Core Server HA
  - Inventory Server
  - Forensic Server
  - Policy Proxy
- Administration Console
  - pybackup.log
  - pyconsole.log
  - pydatabase.log
  - update.log
- Log do personalizador de banco de dados

NOTA: Para navegar por essa tela, use o seguinte:

- Para acessar o final do registro, você pode manter pressionada a tecla alt direita e, em seguida, pressionar "/" no teclado
- Para sair do log, segure a tecla ctrl esquerda e pressione "x" no teclado.
- as teclas de seta permitem a navegação.
- as teclas page up e page down avançam e retrocedem uma página por vez.
- a barra de espaço avança em uma página nos logs.

Abrir a interface da linha de comando

Para abrir a interface de linha de comando, no menu principal, selecione **Iniciar shell**.

Para sair da interface de linha de comando, digite **exit** e pressione **Enter**.

Gerar um log de instantâneos do sistema

Para gerar um log de instantâneo do sistema para o Dell ProSupport, no menu principal, selecione **Ferramentas de suporte**.

1 No menu *Ferramentas de suporte*, selecione **Gerar log de instantâneo de sistema**.
2 Na indicação que o arquivo é criada, selecione **OK**.

3

Manutenção

Remova backups desnecessários do do Servidor de gerenciamento de segurança virtual.

Somente os dez backups mais recentes são retidos. Se o espaço disponível na partição do disco estiver em dez por cento ou menos, não será armazenado mais nenhum backup. Se essa condição ocorrer, você receberá uma notificação por e-mail informando que há pouco espaço de alocação em disco.

4

Solução de Problemas

Se ocorrer um erro e você tiver configurado as notificações de e-mail, você receberá uma notificação por e-mail. Com base nas informações fornecidas pela notificação por e-mail, siga essas etapas:

1 Verifique os arquivos de log aplicáveis.

2 Reinicie os serviços, conforme necessário. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

3 Gerar um log de instantâneos do sistema.

4 Entre em contato com o Dell ProSupport. Para obter mais informações, consulte Entrar em contato com o Dell ProSupport.

5

Post-Installation Configuration

Após a instalação, alguns componentes do seu ambiente poderão precisar ser configurados com base na solução Dell Data Security usada pela sua organização.

Configuração do Data Guardian

Para configurar o Dell Server para suportar Data Guardian, no Management Console, configure um ou ambos os essas políticas para **On**: *Protected Office Documents* and *Cloud Encryption*.

Para obter instruções sobre como instalar o Data Guardian client, consulte o *Guia do administrador* do *Data Guardian* ou o *Guia do usuário do Data Guardian*. É recomendável que os administradores ativem o SMTP para permitir que a Dell Data Guardian envie e-mails para usuários externos, e para permitir o uso de gerenciamento de chaves mais fácil aos criadores.

Validar a verificação de cadeia de confiança do gerenciador

Se um certificado autoassinado for usado no Servidor de gerenciamento de segurança virtual para SED ou BitLocker Manager, a validação de confiança de SSL/TLS precisa permanecer ***desativada*** no computador cliente. Antes de ativar a validação de confiança de SSL/TLS no computador cliente, os seguintes requisitos precisam ser atendidos:

- Um certificado assinado por uma autoridade raiz (por exemplo, Entrust ou Verisign) precisa ser importado para o Dell Server. Consulte Importar um certificado existente ou inscrever um novo certificado de servidor.
- A cadeia completa de confiança do certificado precisa ser armazenada no Microsoft keystore no computador do cliente.

Para desativar a validação de confiança de SSL/TLS no computador cliente, altere o valor da seguinte entrada no registro para 1:

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

DisableSSLCertTrust=REG_DWORD (32-bit):1

Tarefas do Management Console Administrator

Assign Dell Administrator Role

1 Como administrador virtual do Security Management Server, faça login no Management Console: https://server.domain.com:8443/webui/. As credenciais padrão são **superadmin/changeit**.

2 No painel à esquerda, clique em **Populações** > **Domínios**.

3 Clique em um domínio para adicionar um usuário.

4 Na página Detalhes de domínios, clique na guia **Membros**.

5 Clique em **Adicionar usuário**.

6 Insira um filtro para pesquisar o nome de usuário por Nome comum, Nome principal universal ou sAMAccountName. O caractere curinga é *.

Um Nome comum, Nome principal universal e sAMAccountName precisam ser definidos no servidor de diretório corporativo para cada usuário. Se um usuário for membro de um Domínio ou Grupo, mas não for exibido na lista de Membros do Domínio ou do Grupo no gerenciamento, verifique se todos os três nomes estão adequadamente definidos para o usuário no servidor de diretório corporativo.

A consulta pesquisará automaticamente o nome comum e, em seguida, o UPN e o nome sAMAccount até que uma correspondência seja encontrada.

7 Selecione os usuários na *Lista de Usuários do Diretório* para adicionar ao Domínio. Use <Shift><clique> ou <Ctrl><clique> para selecionar múltiplos usuários.

8 Clique em **Adicionar**.

9 A partir da barra de menu, clique na guia **Detalhe e Ações** do usuário específico.

10 Role pela barra de menu e selecione a guia **Admin**.

11 Selecione as funções de administrador que serão adicionadas a este usuário.

12 Clique em **Salvar**.

Fazer login com a Função de Dell Administrator

1 Faça logout do Management Console.

2 Faça login no Management Console e faça login com as credenciais de usuário do domínio.

Clique em "?" no canto superior do Management Console para iniciar a *AdminHelp*. A página *Introdução* é mostrada. Clique em **Adicionar domínio**.

As políticas de linha de base foram definidas para a sua organização, mas estas podem ser modificadas de acordo com as suas necessidades específicas, da seguinte maneira (o licenciamento e os direitos guiam todas as ativações):

- A criptografia com base na política será ativada com criptografia de chave comum
- Computadores com unidades de criptografia automática serão criptografados
- O BitLocker Management não é ativado
- O Advanced Threat Prevention não é ativado
- O Threat Protection é desativado
- A mídia externa não será criptografada
- As portas não serão gerenciadas pelo controle de porta
- Dispositivos com criptografia completa de disco instalada não serão criptografados
- O Data Guardian é desativado

Consulte o tópico AdminHelp *Gerenciar políticas* para obter informações sobre as descrições de políticas.

Confirmar políticas

Confirme as políticas quando a instalação for concluída.

Para confirmar as políticas após a instalação, ou, mais tarde, após as modificações da política serem salvas, sigas estas instruções:

1 No painel à esquerda, clique em **Gerenciamento > Confirmar**.
2 Em *Comentário*, digite uma descrição da alteração.
3 Clique em **Confirmar políticas**.

7

Ports

A tabela a seguir descreve cada componente e sua função.

Nome	Porta padrão	Descrição
Compliance Reporter	HTTP(S)/ 8084	Fornece uma visão completa do ambiente para auditoria e geração de relatórios de conformidade.
Management Console	HTTPS/ 8443	A central de controles e o console de administração da implantação de toda a empresa.
Core Server	HTTPS/ 8887 (fechado)	Gerencia o fluxo de política, as licenças, o registro para Preboot Authentication, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Prevention. Processa os dados de inventário para uso pelo Compliance Reporter e pelo Management Console. Coleta e armazena os dados de autenticação. Controla o acesso baseado em função.
Core Server HA (Alta disponibilidade)	HTTPS/ 8888	Um serviço de alta disponibilidade que permite maior segurança e desempenho das conexões HTTPS com o Management Console, Preboot Authentication, SED Management, FDE, BitLocker Manager, Threat Protection e Advanced Threat Prevention.
Security Server	HTTPS/ 8443	Comunica-se com o Policy Proxy; gerencia as recuperações de chaves forense, ativações de clientes, produtos Data Guardian e comunicação SED-PBA.
Compatibility Server	TCP/ 1099 (fechada)	Um serviço para gerenciar a arquitetura corporativa. Coleta e armazena os dados iniciais de inventário durante a ativação e os dados de política durante as migrações. Processa os dados baseados em grupos de usuário.
Message Broker Service	TCP/ 61616 (fechado) e STOMP/ 61613 (fechada ou, caso configurado para DMZ, porta 61613 aberta)	Lida com a comunicação entre os serviços do Dell Server. Armazena as informações de políticas criadas pelo Compatibility Server para o enfileiramento do Policy Proxy.
Identity Server	8445 (fechado)	Trata as solicitações de autenticação de domínio, incluindo autenticação do SED Management.
Forensic Server	HTTPS/ 8448	Permite que administradores com privilégios adequados obtenham as chaves de criptografia do Management Console para o uso em tarefas de desbloqueio ou descriptografia de dados.

Nome	Porta padrão	Descrição
		Necessário para Forensic API.
Inventory Server	8887	Processa a fila de inventário.
Policy Proxy	TCP/ 8000	Fornece um caminho de comunicação baseado na rede para fornecer atualizações da política de segurança e atualizações de inventário. Necessário para Encryption Enterprise (Windows and Mac)
LDAP	389/636, 3268/3269 RPC - 135, 49125+	Porta 389 – Esta porta é usada para solicitar informações a partir do controlador de domínio local. As solicitações de LDAP enviadas para a porta 389 podem ser usadas para buscar objetos apenas dentro do domínio doméstico do catálogo global. No entanto, o aplicativo de solicitação pode obter todos os atributos para esses objetos. Por exemplo, uma solicitação à porta 389 poderia ser usada para obter um departamento do usuário Porta 3268 – Esta porta é usada para filas especificamente voltadas ao catálogo global. As solicitações de LDAP enviadas para a porta 3268 podem ser usadas para buscar objetos em toda a floresta. No entanto, apenas os atributos marcados para replicação para o catálogo global podem ser devolvidos. Por exemplo, o departamento de um usuário poderia não ser devolvido usando a porta 3268 já que esse atributo não é replicado para o catálogo global.
Client Authentication	HTTPS/ 8449	Permite que os servidores clientes autentiquem com o Dell Server. Necessário para Server Encryption
Sinalizador de retorno de chamada	HTTP/TCP 8446	Em um servidor front-end, permite a inserção de um beacon de retorno de chamada em cada arquivo protegido do Office ao executar o modo Documentos protegidos do Office do Data Guardian.